Online Safeguarding Policy

Last Updated October 2022

Online Safeguarding Statement

The BIT Collective is committed to ensuring a safe environment for all. Online meetings should be just as safe for young people to attend as offline activities. Online as offline, we provide an atmosphere of trust and respect, recognising that young people have a right to protection.

We believe that:

- the welfare and interests of young people are paramount
- all young people who engage with us online have the right to protection from abuse
- all suspicions and allegations of abuse should be taken seriously and responded to swiftly and appropriately
- all staff, contractors and volunteers should be clear as to what constitutes appropriate behaviour and responses and have a responsibility to report concerns

We will ensure that:

- We promote and prioritise the safety and wellbeing of young people who engage with us online regardless of disability, gender, race, religion or belief, nationality or sexual orientation
- We recognise that some young people are additionally vulnerable
- staff understand their role and responsibilities in terms of safeguarding young people online
- Staff are provided with appropriate learning and development opportunities to feel confident and supported in ensuring online safeguarding for all
- Policies and procedures regarding safeguarding responsibilities are available to participants

Introduction to Safeguarding

The term safeguarding is used to define actions taken to protect vulnerable groups from harm. This harm might come from adults or indeed children and, as a consortium of organisations working closely with vulnerable groups, it is important we understand what safeguarding is and why it is important.

Online abuse or exploitation can happen anywhere online that allows digital communication, including:

- Social networks/platforms (Facebook, Instagram/Twitter)
- Text messages and messaging apps (WhatsApp/Kik/Snapchat)
- Email and private messaging (Gmail, Instant messenger)
- Online chat sites/apps (Skype, Zoom, Teams)
- Online streaming sites (YouTube, Instagram)
- Voice chat in games (Playstation/Xbox)

There are many potential risks to children on online. These can come from criminal activity by adults trying to groom children online or from activity by other children. They can include, but are not limited to:

- cyberbullying
- posting personal information that can identify and locate a child offline
- Sexual abuse including, but not limited to, luring, exploitation, grooming and child abuse imagery
- exposure to inappropriate content
- involvement in making or distributing illegal or inappropriate content
- exposure to information and interaction with others who encourage self-harm
- running away from home as a result of contacts made online

Online risk can be classified in three ways:

Content risk: children receiving mass-distributed content. This may expose them to age-inappropriate content such as pornography, extreme violence or content involving hate speech and radicalisation

Conduct risk: children participating in an interactive situation. This involves bullying, harassing, aggression, stalking or promoting harmful behaviour such as self-harm, suicide, illegal drug. The child's own conduct online can also make them vulnerable, for example sharing personal information or bullying and harassing others

Contact risk: children being victims of interactive situations. This includes being bullied, stalked, meeting strangers, threats to privacy, identity and reputation, a house location being identified, someone impersonation a user, violence, threats and abuse

Safeguarding standards on The BIT Collective

The guidance below will outline principles for engaging with young people online through The BIT Collective. This guidance is intended to supplement existing child protection and safeguarding standards approved by the Board, as opposed to replacing previous guidance.

1) Age Ranges

The BIT Collective works with young people aged 11-25. It is important to note that there are different principles relevant to different age groups. The first point to consider is the age of participants that you will engage through your activity.

11-12 Years Old

Young people aged 11-12 **must be engaged via their parents**. This relates to legislation within COPPA - Children's Online Privacy Protection Act

https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

13-18 Years Old

Young people aged between 13-17 years old are considered Children, and all safeguarding measures must be applied. At 13 years old, you are able to access a number of social media channels, including Instagram, Facebook, YouTube. It is important to note that you must be 16 years of age before using WhatsApp.

18+

Individuals aged 18+ will be considered within a separate safeguarding vulnerable adults policy.

2) Risk Assessment

Before undertaking any online activity, you must complete the **E-Safety risk assessment and action plan** and submit to the BIT Collective Safeguarding Team for review.

The primary objective of this document is to protect children from risk online by enabling staff to self-assess online services and inform them of mitigation strategies which must be put in place to reduce the risk of harm to children.

3) Assessing risk across different channels

A key principle of online safeguarding is 'know your channel'. The table below has been created to help assess the risk across different social channels.

Channel	Description	Age Range	Comments
Telegram	Telegram is a messaging app where you can send messages, photos, videos and documents to your contacts, as well as creating group chats of up to 200,000 people. All communications, including voice calls, are end-to-end encrypted.	16+	You can receive messages from people you don't know, so this setting should be turned off.
Instagram	Instagram is a picture and video sharing app. Users can post content on their profile grid or to their stories, which last 24 hours. You can follow your friends, family, celebrities and companies on Instagram. Instagram also has a live streaming feature.	13+	Instagram has geo-location so this should be turned off. Risk of DM's that we can't moderate. You can set an age limit for your page as a business. There are weak age limit checks so we may not be able to ensure age ranges. There can be lots of advertising/spam.

YouTube	YouTube is a video sharing platform. Users can upload videos, comment and like videos, and subscribe to channels.	13+	There are content settings. We need to moderate the comments or disable comments.
Discord	Discord is a voice and text chat app that's popular with gamers. It can be used to talk to other players while playing games.	13+	There are content settings. Private servers can be set up.
Facebook and Messenger	Facebook is a social media app, where people can post, like (pages and posts), comment on and share content. People can add users as friends, and this can occur separately on Facebook and Messenger.	13+	Quite a high-risk platform. There can be lots of advertising/spam. Individual users should be aware of their own privacy settings. Comments can be removed, and users can be blocked. Employees, board members and freelance contractors should not friend any young person on Facebook or Messenger.
Zoom and Teams	Zoom and Teams are video conferencing applications, which can be used to host online events.	16+	Screen recording can be an issue, and permission must be obtained to do so. People can share screens and therefore share inappropriate content. However, settings can ensure only the 'host' can share content. Zoom calls are at risk of 'zoom bombing'. This can be prevented through use of the virtual 'waiting room', and users can be removed by the host.
WhatsApp	WhatsApp is an encrypted messaging application.	16+	There is risk of bullying in group chats. There is no reporting function. Once someone is 'added' on WhatsApp, added users have access to their phone number.

Please note that The BIT Collective delivery will restrict the use of:

- **TikTok**- this platform has insufficient safeguarding principles and is not appropriate for use with/by young people.

Zoom

The BIT Collective's preferred application for online meetings, workshops and seminars is Zoom. Internally hosted and organised Zoom sessions should meet the following safeguarding standards, and where young people are involved in any externally hosted calls, the host should ensure these standards are also met. The BIT Collective's zoom safety standard requires the following security measures to be applied:

- **Only join Zoom meetings when the invite has been sent to you by someone you know**: check the sender's email - there are instances of spoof emails being used to capture user data.
- **Don't share invites**: if you have been sent a personalised invite after registering for a Zoom meeting, do not share it with others. Everyone should register individually
- **Never share your meeting ID**: Each Zoom user is given a permanent 'Personal Meeting ID' (PMI) that is associated with their account. If you give your PMI to someone else, they will always be able to check if there is a meeting in progress and could potentially join
- **Do not post pictures of your Zoom meetings**: If you take a picture of your Zoom meeting then anyone who sees this picture will be able to see its associated meeting ID and can try to access the meeting
- **If you haven't been asked to pre-register for the meeting, ask for:** a password, that waiting rooms have been enabled, that screen sharing is limited, the room is locked once all participants have arrived
- **We advise against joining any event where the actual meeting invite has been shared on a searchable web page or social media:** Posting links to Zoom meetings on crawlable pages that show up in search engines such as Google, or on Social Media, is an invitation for hackers to enter meetings and disrupt them. Advise the host that they should not do this, and if you are joining a call that has been publicly posted, ensure all the above steps have been taken to minimise the risk to yourself and others

4) Core principles for working online

Below is the guidance for using a variety of platforms when communicating with children and vulnerable adults online.

Setting up a meeting

- Fully understand the software you are using
- Meetings must be chaired by an adult
- No one can enter the meeting room without the chair (an adult)
- If you are hosting a regular meeting with similar groups of young people, establish a code of conduct for the meeting
- Under 18's can attend meetings by invite ONLY, and with the signed permission of a parent or guardian
- You must retain a list of children that have been invited to each meeting
- Password protect all meetings and send the password separately to the meeting link
- Have 'waiting room' enabled at all times so that participants have to be admitted to a meeting and cannot just join by 'clicking the link'
- Ensure there is no searchable trace of the meeting e.g., sharing links on social media
- Ensure young people engaging with meetings have been briefed on safeguarding guidance (e.g., if a group are meeting regularly)

Joining the meeting

- Switch the settings to have microphones and videos off when joining the meeting
- Remind users about respecting others and using the chat box for commentary
- Disabled one-on-one communication between participants
- Ensure the host is in control of who can control the screen, save the video/chat content
- Once all participants have joined, lock the meeting
- Encourage participants to use their first name (rather than full name) in their screen name
- Staff should not use their personal emails to join the meeting

During the meeting

- Ensure all participants are able to mute themselves/turn off their video
- If meetings are compromised the chair should close the meeting immediately
- Ensure the chair or an adult is monitoring and moderating the chat
- Learn how to mute and unmute all participants, including video screens
- Be conscious of background environments and others in the room
- Ensure meetings are not recorded when young people are present
- Please dress and talk appropriately
- Do not take photographs of zoom calls
- If a participant needs to leave the call because they are feeling distressed or overwhelmed, they should message a PVG checked volunteer on the call (host-only messaging will be enabled) and they will either be taken into a breakout room or contacted off zoom (phone call) for support.
- If a disclosure is made, the participant will be taken into a breakout room or contacted by phone by a PVG checked volunteer who will provide immediate support in addition to following the “Reporting an Incident” procedures outlined in the Child Protection Policy.
- If the disclosure is made in the session in a way that all participants are aware of it, the remaining PVG checked volunteer(s) will provide immediate support to the remaining participants, which may include: providing information on what will happen next according to the Child Protection Policy (e.g. transparency over due process such as reassurance on what is happening with the person who disclosed); providing space for everyone to process what has happened; providing information on support resources; ending the call early if it is not possible to resume the intended activity.
- If a participant behaves in a way that is inappropriate, they will be immediately taken into a breakout room by an allocated member of The BIT Collective. If it is determined that the inappropriate behaviour was unintended, and that the participant is not deemed a risk to others on the call, they may be readmitted. If it is determined that the inappropriate behaviour was intentional, they will be removed from the call and a review will be carried out to determine whether it is appropriate for them to continue to participate in activities run by the organisation.

5) Live Streaming

Live streaming is a valuable way to connect with the wider community, but you must be aware of children and young people's safety. Below are specific safeguarding recommendations regarding live streaming, as it is expected that this will form a key element of The BIT Collective activity.

If you provide young people with access to live streaming media (e.g., webcams and Skype) use an open area and make sure the activity is observed by appropriate adults. Key safeguarding principles include:

- Talk to children and young people about online safety before the session starts
- Make sure they understand that live streaming is live. Any comments they make will be seen by others and they probably won't be able to delete or edit them
- Remind them not to share any personal information and not to respond to contact requests from people they don't know
- Some live streams request donations from the audience. Explain to children and young people that they don't have to contribute
- Make sure they know who to tell if they see or hear anything upsetting or inappropriate
- Whichever platform you're using, make sure you understand the privacy settings and know how to report any offensive or abusive content
- Never reveal the full identity of individual participants and be sensitive to the needs of those who may have child protection concerns.

Things to consider if you're hosting a live streaming event include:

- Does the platform you're using allow you to restrict the audience, for example by asking them to create a login and password?
- Will other people be able to reproduce and distribute your stream?
- have you got consent for children to participate in the stream?

Things to consider if you're taking part in someone else's live stream include:

- making sure you know what content will be used in the stream and check it will be appropriate for the children and young people who will be watching it
- finding out how the stream will be used in the future, for example if it will be archived or broadcast again.

Safeguarding standards at The BIT Collective

1) Responsibilities

The Safeguarding Team will be responsible for administrative procedures relating to the selection and induction of staff and for advising on any disciplinary action.

Online hosts will monitor the implementation of the policy and take appropriate action on any breaches within their areas of responsibility. They will carry responsibility on an agreed meeting by meeting basis.

It is not the role of the Online Host decide whether a young person has been abused or not – this is the task of the social services department which has this legal responsibility, or of the police.

All staff and contractors engaging with young people online have a responsibility to maintain appropriate standards of behaviour and to report lapses in these standards by others. Any concerns or reasonable suspicions of abuse should be reported to line management.

Any allegations of inappropriate behaviour should also be reported to the BIT Collective Welfare Officer (email bitcollectivewelfare@gmail.com), who will escalate this concern to The BIT Collective Safeguarding teams. You should also escalate this concern within your respective organisation. Please see The BIT Collective's Whistleblowing Policy for further details on how to make a complaint anonymously or confidentially.

2) Disclosures

During online engagement, young people may disclose concerns or issues to the group or hosts. This may be done verbally or using a chat function. The Online Host will apply the following guidelines in responding to online disclosures:

At the point of disclosure: when a young discloses concerns the Online Host will provide immediate support. At the same time, it is important to be aware of the effect disclosures can have on other participants in online groups, and that the young person may not want everyone in the group to be part of this conversation, therefor the following steps should be taken:

- acknowledge; show that you have heard what they are saying, and that you take their allegations seriously
- assess: if the situation requires and urgent response, consider making a quick apology to other participants and then removing them from the group, so you can respond to the young person at risk individually
- encourage the young person to talk; do not prompt or ask leading questions. Don't interrupt when the young person is recalling significant events. Don't make them repeat their account
- explain what actions you must take; do not promise to keep what you have been told secret, as you have a responsibility to disclose information to those who need to know. Reporting concerns is not a betrayal of trust
- support and comfort; be non-judgmental, listen actively and let the young person know that they are not alone. Don't be afraid to give emotional support, often the best support is compassionate listening
- share tools and support the young person can access immediately with them (e.g., signposting)
- do not share your private contact details with the young person

Following the disclosure:

- create a log of the incident, write down what you have been told, using the exact words if possible, make a note of the date, time, place and people who were present/online at the discussion. Do not use the young person's full name, use initials instead. Share this report with The BIT Collective's Welfare Officer (email bitcollectivewelfare@gmail.com).

3) Health Emergencies

During online engagement, young people may accidentally injure themselves or experience a medical emergency. You may witness accidents, injuries or symptoms ranging from non-life-threatening to severe in the video chat or hear alarming noises when the camera is switched off.

The Online Host will apply the following guidelines in responding to medical emergencies witnessed online:

At the point of accident: establish severity, the Online Host will establish if the person is responsive. They will make sure the young person seeks out or receives immediate medical support as necessary. At the same time, it is important to be aware of the effect witnessing accidents can have on other participants in online groups, and that other young people may be affected by what they are witnessing, therefor the following steps should be taken:

- assess; speak to the injured person, establish if they are responsive
- assess: if the situation requires and urgent response, consider making a quick apology to other participants and then removing them from the group, so you can respond to the young person at risk individually
- encourage the young person to seek medical attention; if the young person is responsive and able to make a call, encourage them to call their GP if there is no immediate risk, or if symptoms are severe encourage them to ring 999 for immediate emergency assistance
- if the young person is not responsive, call 999 and provide as many details as you can
- Any medical emergency should be taken seriously. It is better to seek professional medical assistance than to put young people at risk

Young people witnessing the medical emergency:

- remove other young people from the meeting/event
- after the incident, send an email to other young people to reassure them that the event is over and has been resolved
- in the email, ask them what you can do to assist them and be guided by their answer
- be aware that everyone is different and what may seem a small event to one person can be a major event for others

Reporting the incident:

- create a log of the incident, write down what you witnessed and how you responded, make a note of the date, time, place and people who were present/online at the discussion. Do not use the young person's full name, use initials instead. Share this report with The BIT Collective's Welfare Officer (email bitcollectivewelfare@gmail.com).